Parlons du SSE : Le VPN est-il vraiment aussi dangereux que ce que l’on veut dépeindre ?

Bechtle IT Forum | 11.06.2024 | SwissTech Convention Center

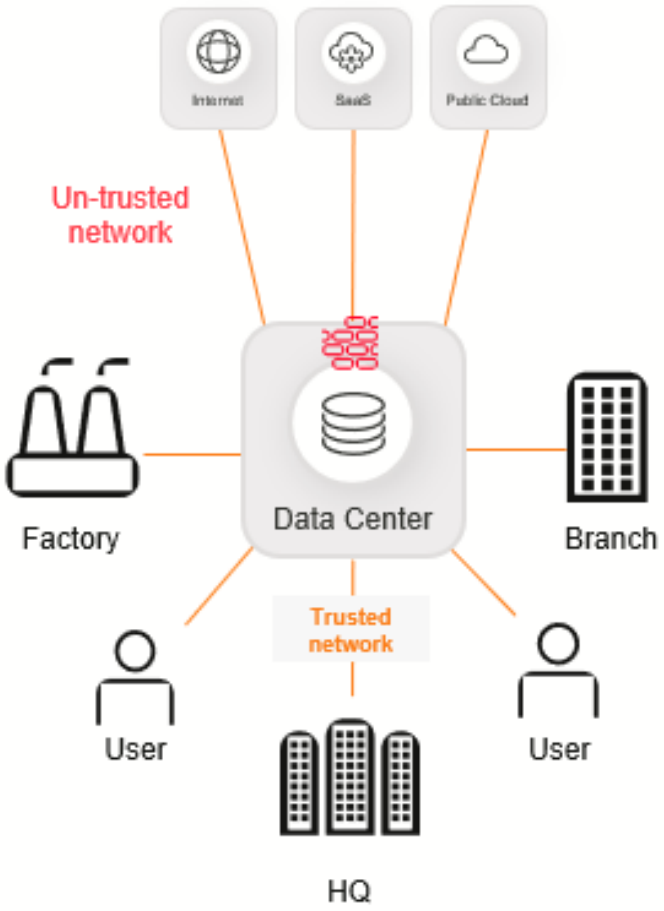
Adrien Morel, Account Manager, HPE Aruba Networking
Luke Berkheiser, Senior Consultant Network, Bechtle Suisse

The modern workplace is **MOBILE**

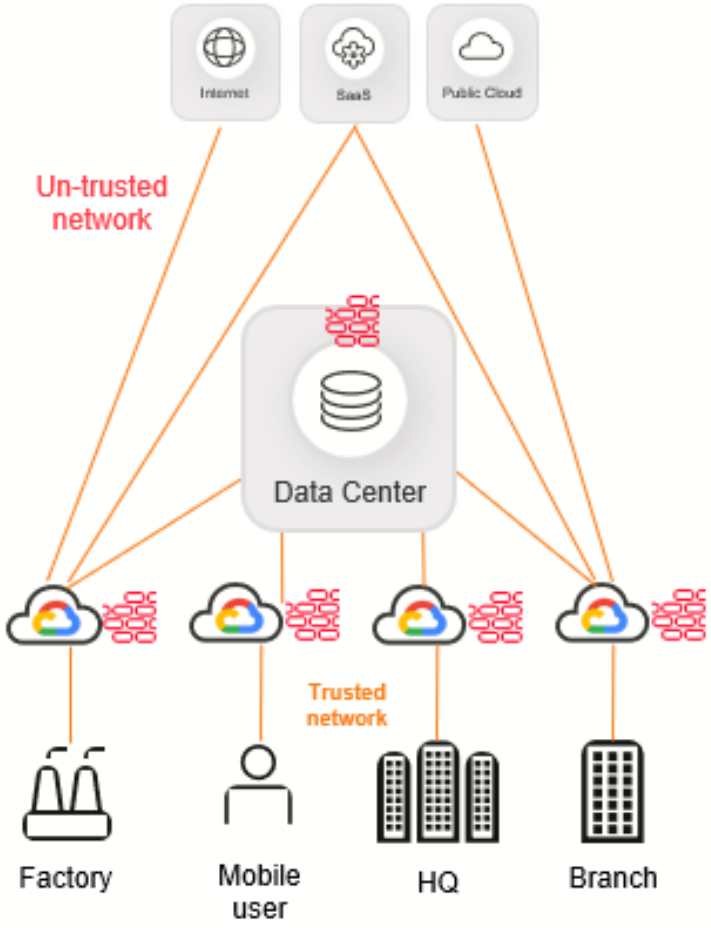
And **95%** of businesses still rely on VPN

Three approaches to secure access

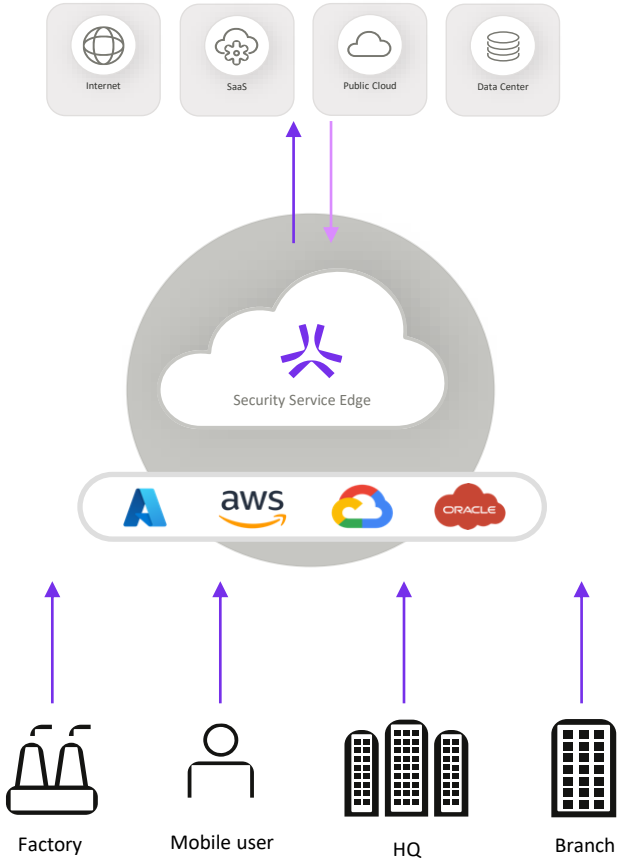
1. Hub and spoke



2. Virtualized cloud firewalls



3. Security Service Edge



The Top 8 VPN Security Risks (What to Look Out for)

VPNs are a great way to protect your Internet traffic and privacy from government surveillance, ISP snooping, and nosy hackers.

But did you know you can also expose yourself to VPN security risks if you're not careful?

TECH > ACTUALITÉS > DONNÉES PERSONNELLES

ALERTES À LA BOMBE: POURQUOI LES VPN N'EMPÊCHENT PAS LES AUTEURS D'ÊTRE RETROUVÉS

Raphaël Grably Le 23/10/2023 à 16:00

CYBER RISKS ASSOCIATED WITH THE USE OF VIRTUAL PRIVATE NETWORKS (VPNs)

Chimaobim Umunna
Experienced Cybersecurity Professional

2 articles + Follo

7 most dangerous VPN security risks

Last updated Apr 12, 2023 at 7am ET · 11

Ethan Payne, Writer

> *While we only consider very few free VPNs as possible alternatives to top-notch premium services, we also have to admit that there is no perfect VPN, either paid or free.*

Obviously, certain VPN security risks are more common in the case of free VPNs, while some may not even relate to paid VPNs. Let's see how a VPN that should protect your anonymity may do just the opposite and risk your virtual as well as your physical security.

Zero-day flaw in Check Point VPNs is 'extremely easy' to exploit

Zack Whittaker · 11:30 AM PDT · May 30, 2024

Comment

Home | Resources | Blog | Remote Access Secu

Zero Trust Access Management

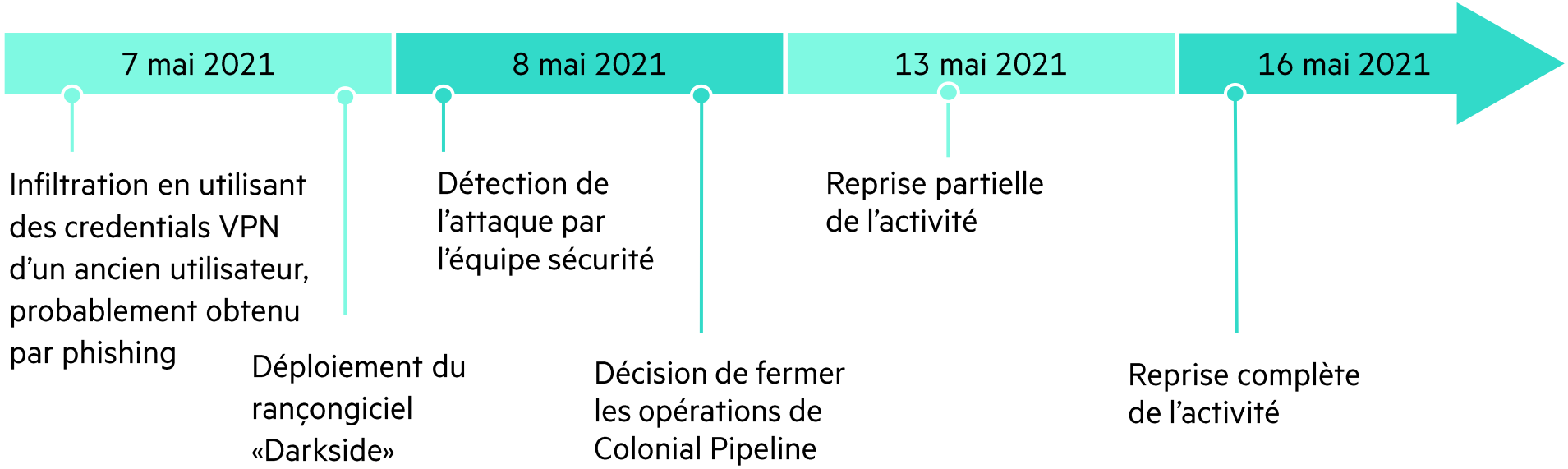
Remote Access Security: The Dangers of VPN

Le VPN, cela date de quand ?

- 1960-1970 : Création du concept de réseau virtuel
- 1996: L’invention du terme "réseau privé virtuel" par l'entreprise Data Encryption Standard (DES)
- Année 2000: Emergence de nouveaux protocoles de VPN modernes (L2TP/Ipsec, Open VPN, etc.)

Le cas de Colonial Pipeline en 2021

Colonial Pipeline Company



- L'attaque a été menée pendant le week-end du Memorial Day, ce qui a pu retarder le temps de réponse de Colonial Pipeline.
- **Pénuries de carburant:** La fermeture du pipeline a entraîné des pénuries de carburant dans plusieurs États de la côte Est, provoquant des files d'attente aux stations-service et une hausse des prix. Colonial Pipeline a initialement versé une rançon de 4,4 millions de dollars aux pirates en échange d'un décrypteur.

Mais concrètement. Lorsque l'on utilise des certificats en plus d'une solution VPN réputée, existe-t-il un risque ?

Et bien pas nécessairement pour les raisons souvent mises en avant…

Mais alors, pourquoi autant de bruit autour du SSE et du VPN ?

Revenons à notre 1ère slide.

- Gartner® a défini en 2019 la notion de SASE.

- Pourquoi ? L'explosion **Work from Anywhere,** ainsi que des **Applications SAAS**

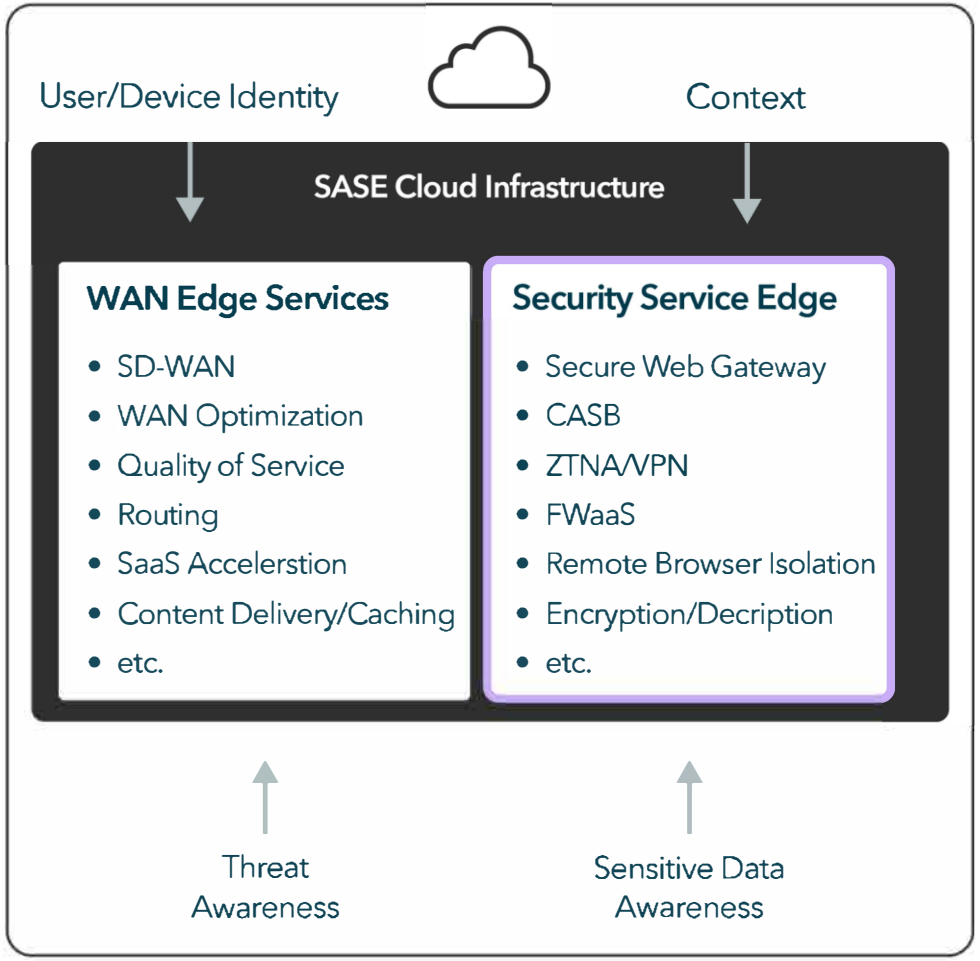
«As of 2019, Secure Access Service Edge (SASE) is a cloud-delivered security service that converges networking (WAN) and security (SWAS) capabilities to provide a unified, consistent, and scalable security architecture for users, devices, applications, and data, regardless of their location» .

- Idée du Gartner d'une potentielle fusion / rapprochement des problématiques de réseau et sécurité.
- Covid / Trop gros step pour les entreprises, alors création en 2021 du sous concept SSE qui se focus uniquement sur la partie Securité du SASE.

- Explosion des applications SAAS utilisées par les employés.

- SSE a été créé en 2021 par … Gartner en retirant la partie SDWAN.
- SSE ne comprend pas la partie networking du SASE.

SASE Architecture



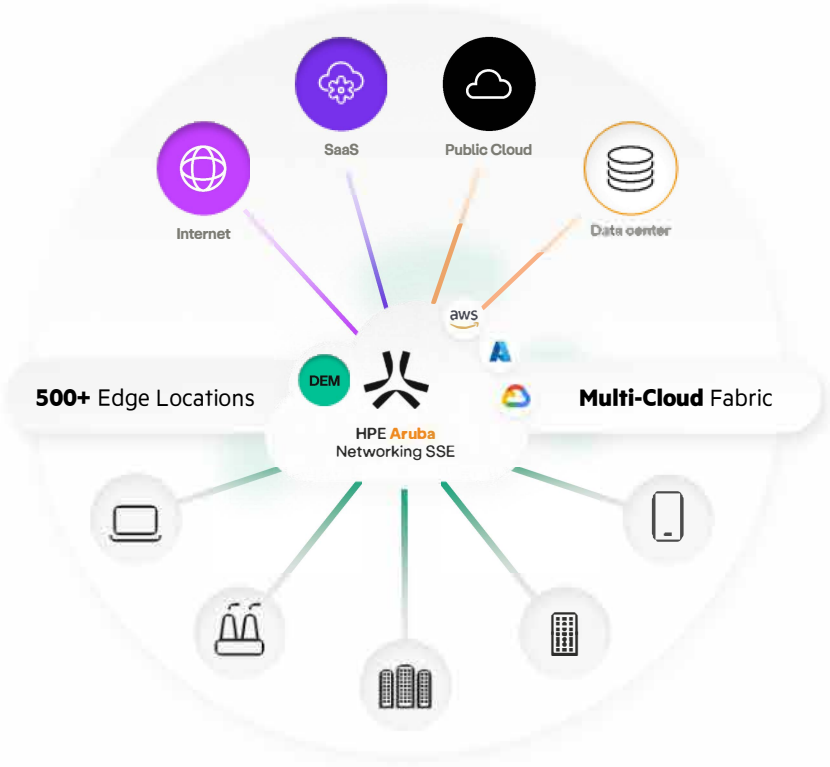
HPE Aruba Networking Security Service Edge (SSE) platform

The 4 pillars of SSE

Zero Trust Network Access

Secure access to private applications in the data center or Cloud.

i.e Minimize app exposure to Internet, remove network access, replace VPN, Inspect traffic, support all private apps



Secure Web Gateway

Secure access to the Internet and protect against malicious online threats.

i.e Filtering, SSL inspection, malware scanning, reputation-based blocking, AI-based Sandboxing

Cloud Access Security Broker

Secure access to SaaS applications and protect against data loss.

i.e Control block upload/download from Box, Sharepoint, Facebook, Salesforce

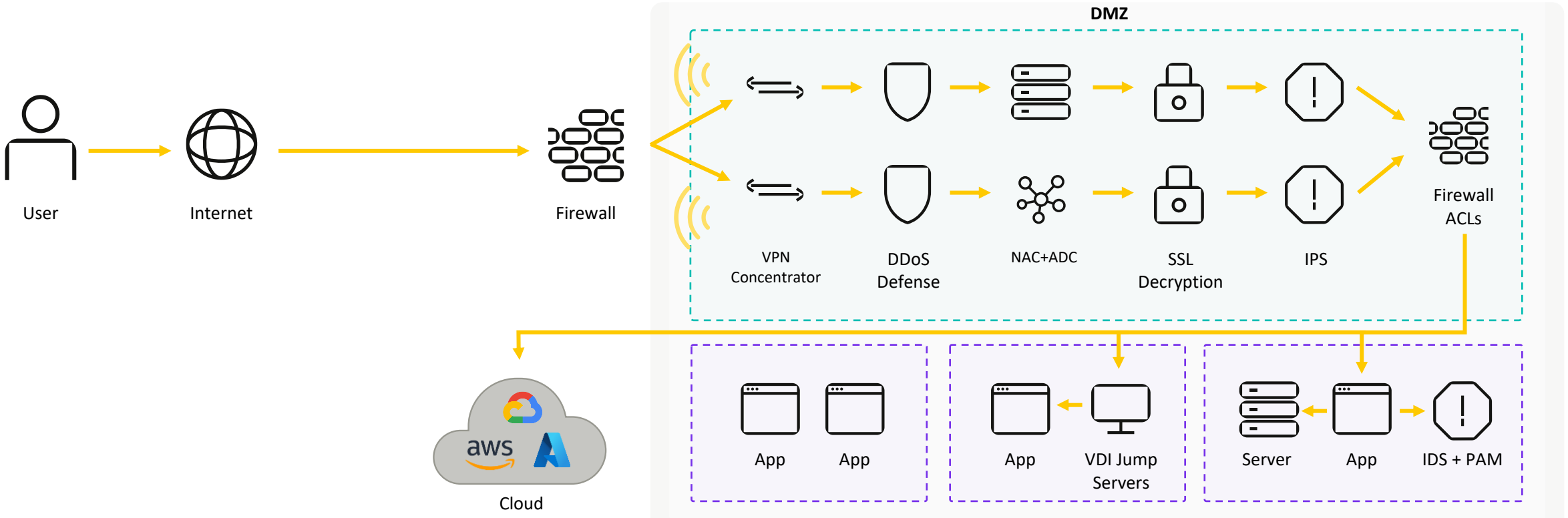
Digital Experience Monitoring

Monitor user performance and to troubleshoot user access issues for all traffic.

i.e Monitor performance of each session, minimize mean time to remediation of user issues

La comparaison VPN / Zero Trust Network Access (ZTNA)

L’exemple de l’accès aux données VPN



VPNs expose IPs

VPNs are like beacons, looking to be found. Consequentially, IPs are exposed creating an attack surface to be exploited.

VPNs over-extend network access

Unknown users from unknown devices are extended network access, increasing attack surface.

VPNs are complex to manage

Scaling physical VPN gateways adds network complexity and is costly.

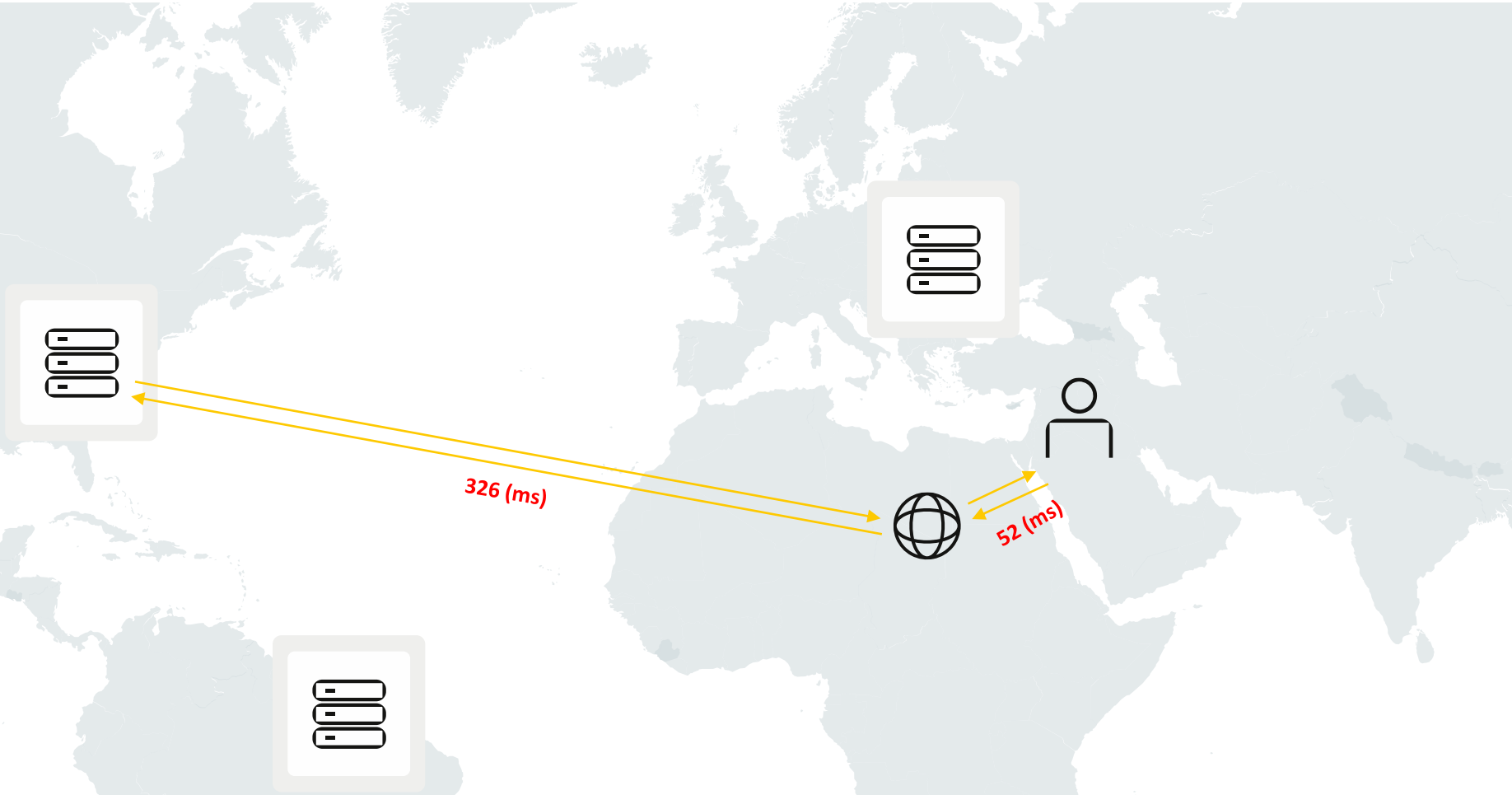
Teams managing multiple configurations and policies across several UI’s is time consuming and error prone.

L’impact de la latence dans le VPN

Over 60% of orgs have 3-6 VPN gateways globally

Traffic is backhauled for miles causing slow connection speed

Users deal with repeated logins and network reconnects

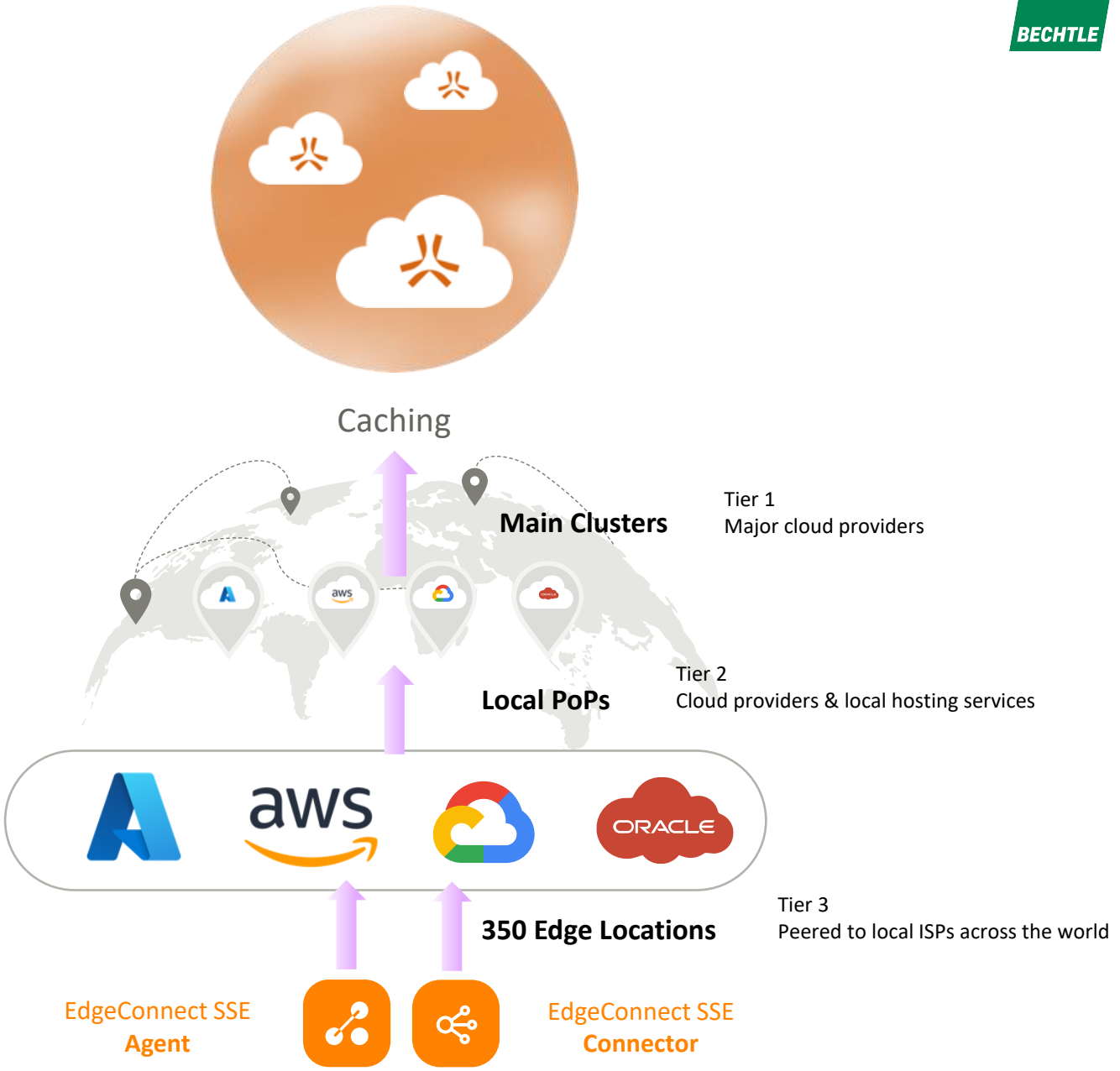


Le cas du SSE

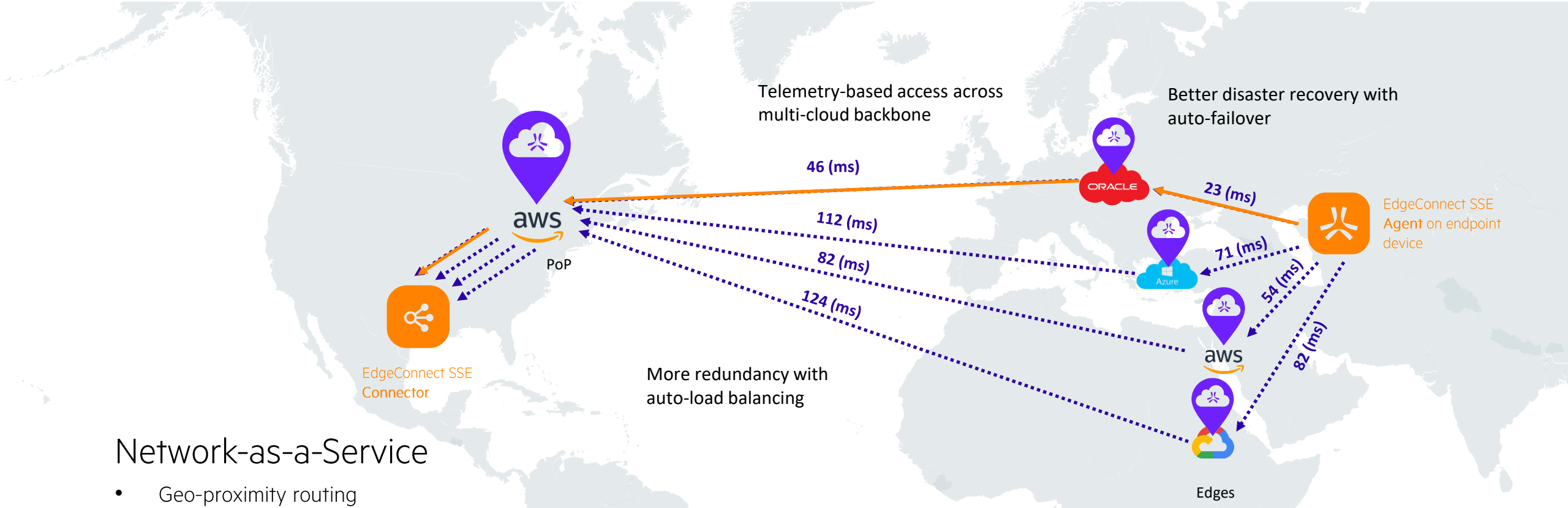
Traffic is never backhauled because of Aruba Cloud architecture's
+350 edges

EdgeConnect SSE automatically chooses the best connectivity path with **smart routing** capabilities

Users receive **continuous access** even if networks change



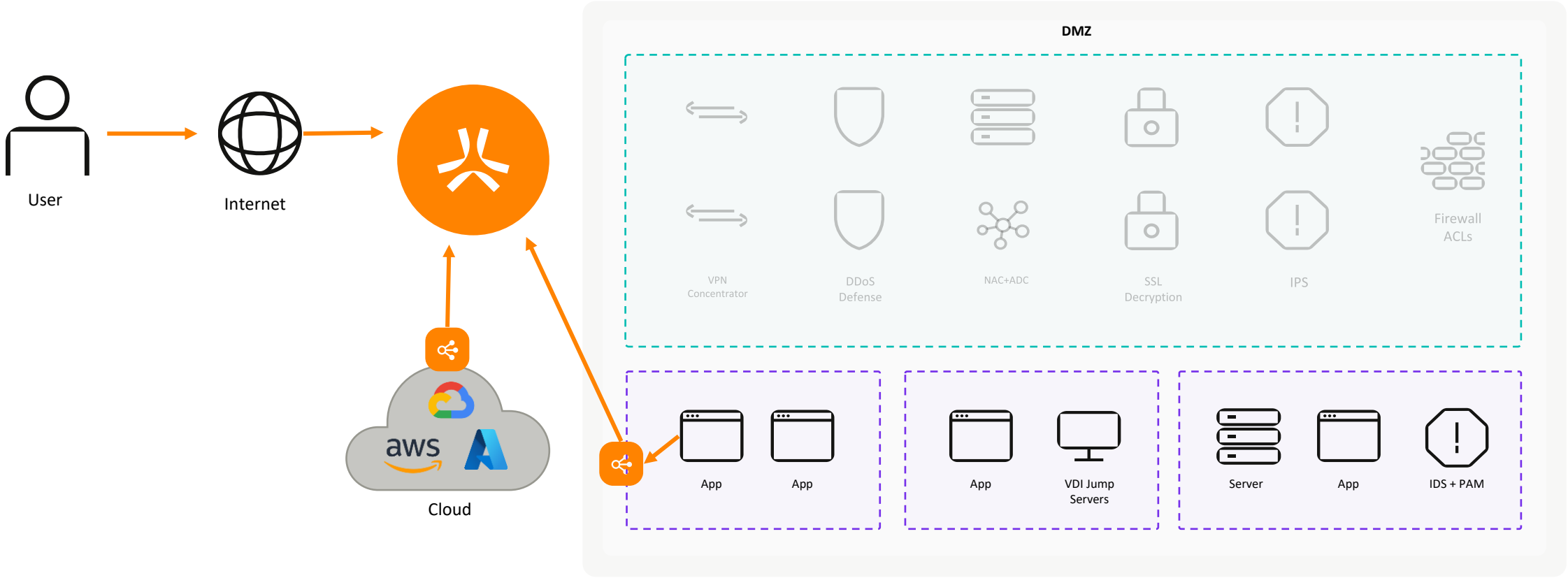
Distributed Cloud Architecture



Network-as-a-Service

- Geo-proximity routing
- Smart routing based on latency
- Extremely high availability

L’exemple de l’accès aux données ZTNA



The invisible network

Inside-out connections make apps completely invisible and never exposed to the internet.

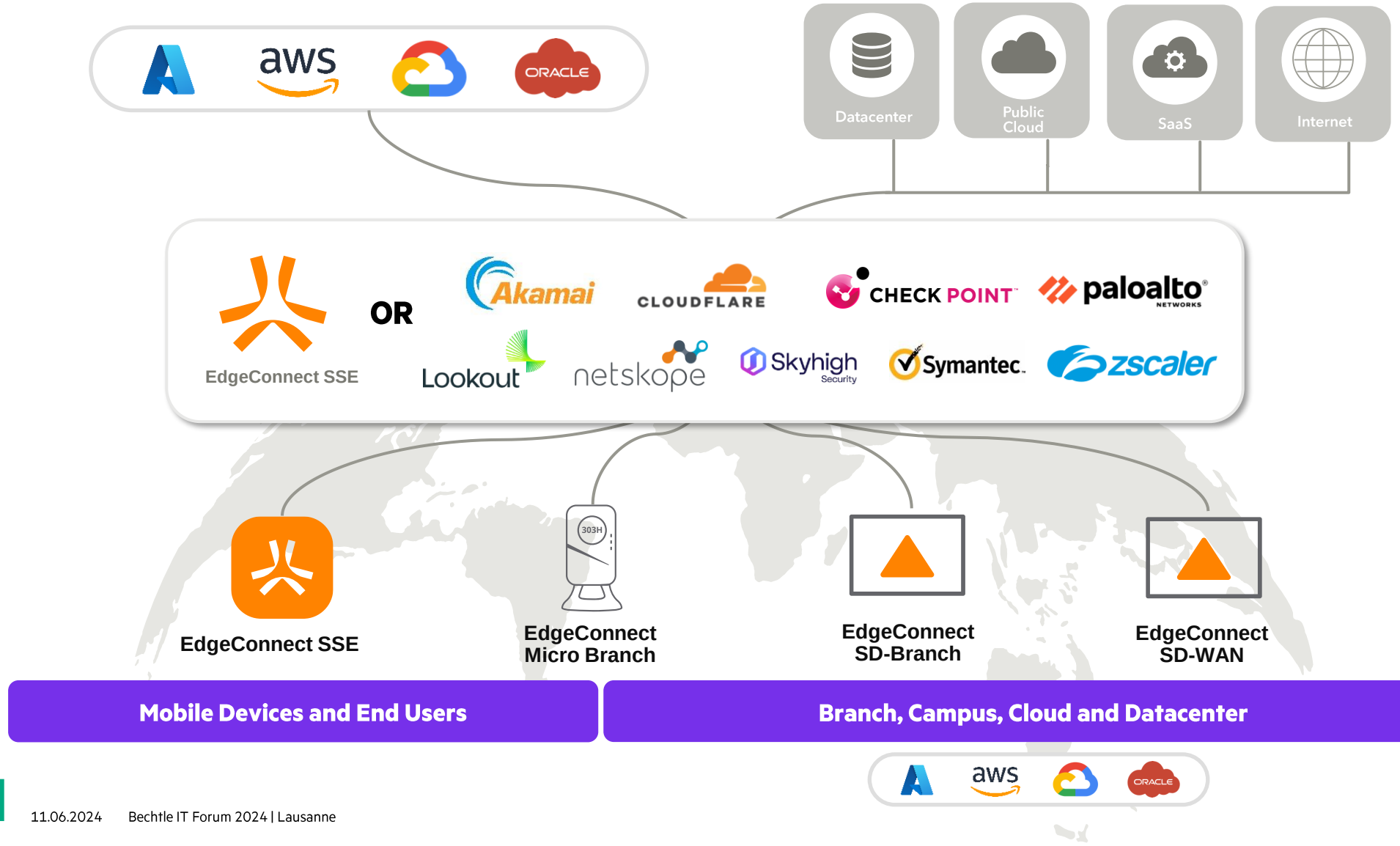
Application access, never network access

Remote users only receive access to authorized applications without placing user or device on the corporate network.

Granular least privilege access.

App-to-user connections provide built-in app segmentation without complex network segmentation. One-to-one connections make lateral movement impossible for unauthorized users.

Fully Integrated SSE or Bring Your Own. We're Open To It.



Merci!

Des questions? Contactez-nous: it-forum.ch@bechtle.com